IN THE UNITED STATES DISTRICT COURT
FOR WESTERN DISTRICT OF TENNESSEE
WESTERN DIVISION

IN THE MATTER OF THE SEARCH AND SEIZURE OF LENOVO LAPTOP BEARING S/N: PF41EM0Z LOCATED AT HSI MEMPHIS, 775 RIDGE LAKE BLVD. STE.300, MEMPHIS, TN	Case No. 24-SW-294

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A WARRANT TO SEARCH AND SEIZE

I, Benjamin W. Grant, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Homeland Security Investigations (HSI) Special Agent (SA) and have been since January 2017. I am currently assigned to the HSI Assistant Special Agent in Charge (ASAC), Memphis, Tennessee. I completed an intensive six-month academy at the Federal Law Enforcement Training Center, located in Glynco, Georgia, which included the Criminal Investigator Training Program and the HSI Special Agent Training Program. While attending the Federal Law Enforcement Training Center I received training in the investigative areas of customs and immigration fraud, child sexual abuse material, human trafficking, narcotics smuggling, money laundering, bulk cash smuggling, the illegal exportation of weapons, munitions and high technology items, the illegal exportation of commodities, general smuggling, and alien smuggling. Before my employment with HSI, I earned a graduate degree from the University of Scranton and served in the U.S. Air Force..

STATUTORY VIOLATIONS

2. Based upon the information contained in this affidavit, I have probable cause to

RL

believe that, located on a Lenovo Laptop bearing S/N: PF41EM0Z (hereinafter SUSPECT DEVICE), there is evidence, fruits, and instrumentalities of violations of federal law, namely 18 U.S.C. § 2252A, possession and distribution of child pornography, and 18 U.S.C. § 2422(b), coercion and enticement as more particularly described in Attachment B.

3. I make this affidavit in support of an application for a warrant to search and seize SUSPECT DEVICE which is in the Western District of Tennessee, described more fully in Attachment A, and to seize the items relating to violations of 18 U.S.C. § 2252A and 18 U.S.C. § 2422 as more fully described in Attachment B.

4. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals participating in this investigation, including other law enforcement officers, my review of documents and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and infornation gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a seizure and search warrant, it does not set forth each and every fact that I or others have learned during this investigation.

DEFINITIONS

5. The below definitions apply to this Affidavit and Attachment B to this Affidavit.

6. "Child Pornography" includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or

B6

modified to appear that an identifiable minor is engaged in sexually explicit conduct).

7. "Visual depictions" includes prints, copies of visual images, developed and undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

8. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

9. "IP Address" means Internet Protocol address, which is a unique numeric address used by computers on the Internet. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

10. "Internet" means a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

11. In this affidavit, the terms "computers" or "digital storage media" or "digital storage devices" may be used interchangeably, and are intended to include any physical object upon which computer data can be recorded as well as all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices capable of performing logical, arithmetic, or storage functions, including desktop and laptop computers, mobile phones, tablets, server computers, game consoles, network hardware, hard disk drives, RAM, floppy disks, flash memory, CDs,

BG

DVDs, and other magnetic or optical storage media.

SEARCH AND SEIZURE OF COMPUTERS

12. As described above and in Attachment B, I submit there is probable cause to search and seize SUSPECT DEVICE for the reasons stated below. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis. They may be searched and seized on-scene, and/or searched off-scene in a controlled environment.

13. For example, based on my knowledge, training, and experience, I know that a powered-on computer maintains volatile data. Volatile data can be defined as active information temporarily reflecting a computer's current state including registers, caches, physical and virtual memory, network connections, network shares, running processes, disks (floppy, tape and/or CD-ROM), and printing activity. Collected volatile data may contain such information as opened files, connections to other computers, passwords used for encryption, the presence of anti-forensic tools, or the presence of programs loaded in memory that would otherwise go unnoticed. Volatile data and its corresponding evidentiary value is lost when a computer is powered-off and unplugged.

14. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, deleted

R6

files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

15. Also, based on my training and experience, wholly apart from user-generated files, computer storage media contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, virtual memory "swap" or paging files, and shadow copies of previous versions of systems or files, or paging files. Computer users typically do not erase or delete this evidence because special software is typically required for that task. However, it is technically possible to delete this information. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted, edited, moved, or show a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

16. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how computers were used, why they were used, the purpose

RG

of their use, and the purposes to which they were put, who used them, the state of mind of the user(s), and when they were used.

17. Information or files related to the crimes described herein are often obtained from the Internet or the cellular data networks using application software which often leaves files, logs or file remnants which would tend to show the identity of the person engaging in the conduct as well as the method of location or creation of the images, search terms used, exchange, transfer, distribution, possession, or origin of the files. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

18. "User attribution" evidence can also be found on a computer and is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, videos, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time. For example, I know from training and experience that persons trading in, receiving, transporting, distributing, or possessing images involving the sexual exploitation of children or those interested in the firsthand sexual exploitation of children often communicate with others through correspondence or other documents which could tend to identify the origin and possessor of the images as well as provide evidence of a

person's interest in child pornography or child sexual exploitation. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

19. Searching computer(s) for the evidence described in the attachment may require a range of data analysis techniques. For example, information regarding user attribution or Internet use is in various operating system log files that are not easily located or reviewed. Or a person engaged in criminal activity will attempt to conceal evidence of the activity by "hiding" files or giving them deceptive names. As explained above, because the warrant calls for records of how a computer has been used, what it has been used for, and who has used it, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of SUSPECT DEVICE for the things described in this warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use a multitude of techniques, both on and off-scene, including more thorough techniques.

20. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes involving child exploitation, they should all be seized as such.

D/

21. Based on my training and experience, I know that a thorough search for information stored in digital storage media requires a variety of techniques that often includes both on-site seizure and search as well as a more thorough review off-site review in a controlled environment. This variety of techniques is required, and often agents must seize most or all storage media to be searched on-scene and/or later in a controlled environment. These techniques are often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction.

22. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include off-site techniques since it is often necessary that some computer equipment, peripherals, instructions, and software be seized and examined off-site and in a controlled environment. This is true because of the below.

a. The nature of evidence. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how, when, and why a computer has been used, by whom, what it has been used for, requires considerable time, and taking that much time on premises could be unreasonable. Also, because computer evidence is extremely vulnerable to tampering and destruction (both from external sources and from code embedded in the system as a "booby-trap"), the controlled environment of a laboratory may be essential to its complete and accurate analysis. Searching for and attempting to recover any deleted, hidden, or encrypted data may be required to determine whether data falls within the list of items to be seized as set forth herein (for example, data that is encrypted and unreadable may not be returned unless law

RL

enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of child exploitation offenses).

b. The volume of evidence and time required for an examination. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Reviewing information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

c. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

RL

d. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

e. Need to review evidence over time and to maintain entirety of evidence. I recognize the prudence requisite in reviewing and preserving in its original form only such records applicable to the violations of law described in this Affidavit and in Attachment B in order to prevent unnecessary invasion of privacy and overbroad searches. I advise it would be impractical and infeasible for the Government to review the mirrored images of digital devices that are copied as a result of a search warrant issued pursuant to this Application during a single analysis. I have learned through practical experience that various pieces of evidence retrieved from digital devices in investigations of this sort often have unknown probative value and linkage to other pieces of evidence in the investigation until they are considered within the fluid, active, and ongoing investigation of the whole as it develops. In other words, the weight of each individual piece of the data fluctuates based upon additional investigative measures undertaken, other documents under review and incorporation of evidence into a consolidated whole. Analysis is content-relational, and the importance of any associated data may grow whenever further analysis is performed. The full scope and meaning of the whole of the data is lost if each piece is observed individually, and not in sum. Due to the interrelation and correlation between pieces of an investigation as that investigation continues, looking at one piece of information may lose its full evidentiary value if it is related to another piece of information, yet its complement is not preserved along with the original.

DI

In the past, I have reviewed activity and data on digital devices pursuant to search warrants in the course of ongoing criminal investigations. I have learned from that experience, as well as other investigative efforts, that multiple reviews of the data at different times is necessary to understand the full value of the information contained therein, and to determine whether it is within the scope of the items sought in Attachment B. In order to obtain the full picture and meaning of the data from the information sought in Attachments A and B of this application, the Government would need to maintain access to all of the resultant data, as the completeness and potential of probative value of the data must be assessed within the full scope of the investigation. As such, I respectfully request the ability to maintain the whole of the data obtained as a result of the search warrant, and to maintain and to review the data in the control and custody of the Government and law enforcement at times deemed necessary during the investigation, rather than minimize the content to certain communications deemed important at one time. As with all evidence, the Government will maintain the evidence and mirror images of the evidence in its custody and control, without alteration, amendment, or access by persons unrelated to the investigation.

23. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for permits both on-site seizing, imaging and searching as well as off-site imaging and searching of storage media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later and perhaps repeated examination consistent with

the warrant. The examination may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

24. Because this warrant seeks only permission to examine the device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the court to authorize execution of the warrant at any time in the day or night.

INVESTIGATION

25. On April 4, 2024, I learned information indicating Kiersten NAPODANO, a registered sex offender, was engaged in a sexual relationship with an identified minor victim (MV). The information I received also indicated that on April 4, 2024, NAPODANO and MV were possibly alone together in a vehicle. I coordinated with the Shelby County Sheriff's Office (SCSO) in an attempt to locate MV and NAPODANO.

26. Later the same day, SCSO encountered MV and NAPODANO in a Toyota sedan which was stopped after running a stop sign. MV, a 17-year-old with no driver license, was discovered operating the vehicle and NAPODANO was in the passenger seat. NAPODANO is a registered owner of the vehicle. I arrived on scene shortly thereafter.

27. I encountered MV at the scene and identified myself as a Special Agent with Homeland Security Investigations. MV provided the below statements in summary and not verbatim.

- MV stated the reason for being stopped was because MV did not fully stop at the stop sign and that they had no license.
- MV stated they were not in school because they did not want to go that day.

- MV stated the reason he was driving was because NAPODANO wanted to apply her makeup (SA note: NAPODANO did not appear to be wearing makeup).
- MV stated they were aware NAPODANO was a sex offender and that NAPODANO had disclosed that fact.
- MV stated they met NAPODANO approximately in December 2023, they talk and have each other's phone number.
- MV displayed NAPODANO's contact on their phone. It was saved as "Neida" a name MV said he gave her.
- MV stated he only calls and never texts NAPODANO or use social media with her.
- MV did not consent to a search of the "hidden images" album on their iPhone.
- MV stated NAPODANO knew he was a minor, 17 years old.
- MV denied having sexual contact with NAPODANO. MV stated they did not want to get NAPODANO in trouble and asked what was going to happen to her.

28. I also encountered NAPODANO at the scene and identified myself as a Special Agent with Homeland Security Investigations. I Mirandized her and asked if she was willing to speak with me. NAPODANO provided the below statements in summary and not verbatim.

- NAPODANO stated the driver was MV and identified them by their true first name.
- NAPODANO stated she does not have a license either but was giving him a ride.
- NAPODANO stated MV did not go to school that morning but that she was driving MV to school now (approximately 2pm) for a party or baby shower.
- NAPODANO was unable or unwilling to explain when and where she picked up MV on April 4, 2024.
- NAPODANO was unable or unwilling to provide a timeline of her day on April 4,

DC

2024.

- NAPODANO stated she first met MV in January or February 2024 at an identified Memphis restaurant where they are employed.
- NAPODANO stated MV contacted her on April 4, 2024, via a Snapchat phone call and she picked him up.
- NAPODANO denied being under the influence of drugs or alcohol and stated the last time she used was four days prior.
- NAPODANO stated she took full responsibility for having MV drive unlicensed.
- NAPODANO denied having sexual contact with MV.
- NAPODANO denied consent to search her phone.
- NAPODANO stated nobody she knows, also knows MV.

29. MV was released from the scene to the custody of their mother. NAPODANO was charged by SCSO with violating the terms of her probation and transported to 201 Poplar.

30. On April 5, 2024, an identified source contacted me and stated they possessed SUSPECT DEVICE (said to be NAPODANO's Lenovo laptop.) The source stated NAPODANO wanted incriminating images to be removed from her devices and her iCloud account (SUSPECT ACCOUNT) to be wiped. They stated they wanted to turn it over because it contained evidence of NAPODANO being a predator. This information was corroborated by NAPODANO's first jail call. At approximately 7:20pm on the day of her arrest, she called an identified person. Their conversation included the following non-verbatim statements made by NAPODANO. Approximately two minutes into her call, NAPODANO stated this is really, really important and I have to be limited on what I say. She stated her iCloud login name and password to the person and directed them to navigate to her Find My app, locate the option as if her device was stolen and

QL

erase all data. NAPODANO stated would you please do that; it's serious. Go in Find My and erase all data as fast as you can.

31. On April 5, 2024, I met with the identified source, and they turned over SUSPECT DEVICE (S/N: PF41EM0Z) and signed a property receipt. During this meeting, the source displayed sexual images on SUSPECT DEVICE to me. The images were displayed voluntarily and unprompted by me. I observed images that showed a male and female engaged in genital-genital penetration. The source stated the female is NAPODANO and the male is MV. I did not observed images with faces. The source stated the images they displayed and other information were linked to NAPODANO's Apple ID. The source also displayed NAPODANO's Apple ID on the device and I observed KIERSTENNAPODANO@GMAIL.COM (SUSPECT ACCOUNT).

32. Given the information referenced in paragraphs 25 through 28, I determined NAPODANO is a registered sex offender who was discovered alone with an identified minor in violation of her status. Given the fact pattern of this case and the information referenced in paragraphs 30 and 31, I determined the images I observed on SUSPECT DEVICE probably constitute child pornography as defined in 18 U.S.C. § 2256 and that the images are probably stored on and or associated with SUSPECT ACCOUNT.

CONCLUSION

33. I submit that there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A and 18 U.S.C. § 2422(b) on SUSPECT

DEVICE described in Attachment A. I, therefore, request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

Respectfully submitted.

Benjamin W. Grant
Special Agent, HSI

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 41 by telephone, this 11th day of July, 2024.

s/Tu M. Pham

HON. TU M. PHAM
Chief United States Magistrate Judge